STATE of ARIZONA

Government Information Technology Agency	Statewide STANDARD P100-S102	TITLE: Platform Infrastructure Effective Date: September 30, 2002

1. AUTHORITY

The Government Information Technology Agency (GITA) shall develop, implement and maintain a coordinated statewide plan for information technology (A.R.S. § 41-3504(A (1))), including, the adoption of statewide technical, coordination, and security standards (A.R.S. § 41-3504(A (1(a)))).

2. PURPOSE

The purpose of this standard is to coordinate agency and State implementations of target platform infrastructure(s). This standard promotes the implementation of platforms that incorporate open systems architecture and proven, pervasive or industry-wide standards. It has been developed in support of the fair competition laws of Arizona, A.R.S. § 41-2565, by providing a range of target platforms throughout the product lifecycle from emergence, through target, to transitional, and finally obsolescence.

3. SCOPE

This applies to all budget units. Budget unit is defined as a department, commission, board, institution or other agency of the state organization receiving, expending or disbursing state funds or incurring obligations of the state including the board of regents and the state board of directors for community colleges but excluding the universities under the jurisdiction of the board of regents and the community colleges under their respective jurisdictions and the legislative or judicial branches. A.R.S. § 41-3501(2).

The Budget Unit Chief Executive Officer (CEO), working in conjunction with the Budget Unit Chief Information Officer (CIO), shall be responsible for ensuring the effective implementation of Statewide Information Technology PSPs within each Agency.

4. STANDARD

The term "platform" applies to servers, storage, and client devices with their respective operating systems, interfaces, and drivers that provide a framework for interoperability, scalability, and portability. Open systems architecture for platforms will further promote the sharing of information/data and other IT resources in support of E-government initiative and programs.

A ***Target Platform Architecture Assessment,*** Attachment A, identifies requirements for the versatility, operating systems, security, and open standard interfaces / drivers that are critical to platform technologies. The ***State of Arizona "As-Is" Platform Assessment***, Attachment B, depicts the platforms installed throughout State agencies, as reviewed and approved by the State CIO and CIO Council.

Target platform architecture must incorporate a range or requirements since at any point in time, given the dynamic nature of the information technology industry and platform-product life cycles, a particular target platform device may no longer completely comply with all requirements. This approach allows agencies to maximize their current investment in certain devices and services, as well as to develop a transition plan to allow obsolete or non-conforming platform elements to be phased out. The intent of the following standards is to specify requirements while allowing a reasonable scoring range, using the assessment tool, for target platform compliance.

4.1. **Versatility:** The device shall be flexible, adaptable, and scalable to provide for new and expanding service requirements.

- Capability shall exist for achieving applicable architecture targets without requiring major upgrades and additional costs.
- Capability shall exist for delivering and/or providing secure (as defined in Statewide Information Security Policy P800 and related standards documents) end-user interface access to a variety of business applications without necessitating substantial modifications, regardless of end-user location.
    - ° Applications include, but are not limited to, e-mail, human resources information systems (HRIS), financial management systems (FMS), Internet, office productivity software, telephony, and voice mail.
- Capability shall exist for delivering and/or providing end-user interface access to a wide variety of business applications using a fully converged network, regardless of end-user location.
- Target Network Architecture standards shall be maximized in the connectivity of devices.
- The device shall be scalable, without substantial modification, to allow for increased demands for services and new applications.
- Widespread choices for off-the-shelf application solutions, without modifications, shall be available for the device.
- The versatility of the device shall directly improve the quality and timeliness of agency business functions.

4.2. **Operating System:** The device shall utilize either an open, industry-standard, secure operating system or a pervasive, industry-standard, secure operating system.

- The open or industry de-facto standard operating system currently installed shall be available for all similar devices offered by the manufacturer.
- The operating system shall provide for updates to be pushed to, or accepted by, all associated devices.
- The device shall be capable or efficiently running the most current production operating system recommended manufacturer; the version installed shall be no more than one major revision behind the most current available version.

- Future production releases of the operating system shall be scheduled by the manufacturer at the time of implementation.

4.3. **Operating System Security:** The device shall have an appropriate, as determined by the agency, level of security functionality incorporated as part of the installed operating system.

- Operating system security services, including access, authentication, and authorization techniques, shall align with the Target Security Architecture and should utilize open standards, where possible.
- Logging and security controls for applications, platform, and network levels shall be integrated to eliminate, or at least reduce, redundancies.
- Support for integrated LDAP-based directory services shall be available.
- Disabling of security options shall be prevented at the user level.
- Security updates from the operating system shall be capable of being pushed to, or accepted by, all associated devices.
- Logging and restriction (including prevention of end-user override) of particular functions and services shall be enabled, including:
  - Non-essential or redundant services,
  - Any communication options susceptible to or prone to abuse, and
  - Utilities at the operating system level.
- Removals of extraneous services, open ports, etc., shall be enabled from default installations of the operating system, and prevented from returning during subsequent upgrades.

4.4. **Interfaces:** The device shall be capable of adhering to applicable, open-system-standard, interface specifications.

- Open-systems standards for any particular interface shall be available and in use.
- Management using standard SNMP-based management tools shall be enabled.
- Network communication protocols shall conform to Arizona's Network Infrastructure Standards, P100-S101.
- Off-the-shelf devices and peripherals conforming to open-systems standards shall be readily obtainable.

4.5. **Drivers:** The device shall be capable of utilizing input/output (I/O) drivers that incorporate IEEE-standard interfacing and industry de-facto standard software drivers.

- Multiple peripheral devices using open-standard drivers shall be available.
- Off-the-shelf peripherals that conform to open system standards shall be readily available.

4.6. **"As-Is" Platform Assessment Ratings:** Given the dynamic nature of target platform lifecycles and advances in the information technology industry, changes to the Arizona "As-Is" Platform Assessment table are inevitable.

- When an agency plans to implement a platform not included on the current Arizona "As-Is" Platform Assessment table (shown in Attachment B) but considered to be an open, industry standard or de-facto industry standard, the CIO shall submit a Target Platform Architecture Assessment (Attachment A) to GITA either in advance of or concurrent with the PIJ.
- Requests for changes to platform ratings shall come from Agency CIOs via submittal to GITA of a completed Target Platform Architecture Assessment (Attachment A) for the item requiring change.
- Arizona's State CIO in conjunction with the CIO Council shall have final approval of all platform assessment ratings, whether conducted virtually or at a CIO Council meeting.

5. DEFINITIONS AND ABBREVIATIONS

Refer to the PSP Glossary of Terms for definitions and abbreviations.

6. REFERENCES

6.1. A. R. S. § 41-621 et seq., "Purchase of Insurance; coverage; limitations, exclusions; definitions."
6.2. A. R. S. § 41-1335 ((A (6 & 7))),"State Agency Information."
6.3. A. R. S. § 41-1339 (A),"Depository of State Archives."
6.4. A. R. S. § 41-1461, "Definitions."
6.5. A. R. S. § 41-1463, "Discrimination; unlawful practices; definition."
6.6. A. R. S. § 41-1492 et seq., "Prohibition of Discrimination by Public Entities."
6.7. A. R. S. § 41-2501 et seq., "Arizona Procurement Code, Applicability."
6.8. A. R. S. § 41-2565, "Specifications, Maximum Practicable Competition."
6.9. A. R. S. § 41-3501, "Definitions."
6.10. A. R. S. § 41-3504, "Powers and Duties of the Agency."
6.11. A. R. S. § 41-3521, "Information Technology Authorization Committee; members; terms; duties; compensation; definition."
6.12. A. R. S. § 44-7041, "Governmental Electronic Records."
6.13. Arizona Administrative Code, Title 2, Chapter 7, "Department of Administration Finance Division, Purchasing Office."
6.14. Arizona Administrative Code, Title 2, Chapter 10, "Department of Administration Risk Management Section."
6.15. Arizona Administrative Code, Title 2, Chapter 18, "Government Information Technology Agency."
6.16. Statewide Information Technology Policy P100.
6.17. Network Infrastructure Standards P100-S101
6.18. Statewide Information Security Policy P800 and related information security standards.
6.19. State of Arizona Target Network Architecture, http://gita.state.az.us/enterprise_architecture.
6.20. State of Arizona Target Security Architecture, http://gita.state.az.us/enterprise_architecture.

6.21. State of Arizona Target Platform Architecture, http://gita.state.az.us/enterprise_architecture.

7. ATTACHMENTS

Attachment A – "Target Platform Architecture Assessment"
Attachment B – "State of Arizona 'As-Is' Platform Assessment"

ATTACHMENT A. TARGET PLATFORM ARCHITECTURE ASSESSMENT

This assessment is designed to support the planning and implementation of Target Platform Architecture recommended standards and best practices. The assessment applies to IT projects that include business requirements that propose or require modifications and/or additions to existing deployments of platform devices.

Score. *Questions for the four (4) platform device categories are scored with one (1) point for a "Yes" answer, and zero (0) for a "No" answer. Maximum possible is the total number of questions for each category.*

> ***Applicable*** *is defined as pertinent, related to, relevant, and appropriate.*
> ***Capability*** *is the potential and ability for development or use. It is the capacity to be used or developed for a purpose.*
> ***Device*** *includes logical groupings or categories of server, storage, and client platforms in use statewide, or within an agency.*
> ***Maximize*** *is defined as taking full advantage of the subject attribute(s).*
> ***Variety*** *is defined simply as more than one. Note: the intent of versatility is to maximize flexibility and usefulness of a device relative to the applicable agency business applications.*
> ***Widespread*** *is defined as extensive and prevalent.*

Platform Device Name/Description:_____

Category	Max. Possible	Score	Category Description
1. Versatility	8		Provides flexibility, adaptability, and scalability without requiring substantial modification.
2. Operating Systems	6		Utilizes open- or pervasive-industry-standard, secure, operating systems.
3. Operating Systems Security	7		Addresses the security functionality of Operating Systems.
4. Open Standard Interfaces & Drivers	4		Adheres to open-system-standard interface specifications and utilizes device drivers with IEEE interfacing and industry de-facto standard protocols and formats.
Total Rating Points	25		

1. Versatility refers to a device's capability (assuming connectivity where applicable) to provide interoperability, flexibility, adaptability, and scalability without requiring substantial modification.

Score 1 Rating Point for a "Yes" answer	Yes
1. Is the device capable of delivering applicable EA Target standards without major upgrades and additional costs?	
2. Is the device capable of delivering or providing secure (as defined by the AZ EA Target Security Architecture) end-user interface access to a variety of business applications (HRIS, email, office productivity applications, Internet, telephony, voice mail, etc.) without substantial modifications, regardless of end-user location?	
3. Is the device capable of delivering or providing end-user interface access to a variety of business applications maximizing a fully converged network, regardless of end-user location?	
4a. Server only – is the device capable of hosting or delivering multiple, and varied, application solutions with sufficient reliability, redundancy, and fault tolerance to support essential agency business operations?	
4b. Storage only – is the device capable of hosting or delivering storage for multiple, and varied, application solutions with sufficient reliability, redundancy, and fault tolerance to support essential agency business operations?	
4c. Client only – is the device capable of providing one common point for end-user connectivity access and productivity for multiple and varied application solutions?	

5. Is the device able to maximize the use of the EA Target Network Architecture standards?	
6. Is the device capable of accommodating increased demands for service and new application solutions without substantial modifications?	
7. Are widespread choices for off-the-shelf application solutions, without modifications, available for this device?	
8. Does the versatility of this device directly improve the quality and timeliness of agency business functions?	
Total Rating Points	

2. Operating Systems refers to a device's, or network's, capability to utilize open- or pervasive-industry-standard operating systems.

Score 1 Rating Point for a "Yes" answer	**Yes**
1. Is an open-industry-standard operating system currently available for this device?	
2. Is the operating system currently deployed with this device an open or industry de-facto standard operating system?	
3. Does the operating system currently deployed with this device allow for all updates to be pushed to, or accepted by, all associated devices?	
4. Is the same version of the operating system currently deployed with this device available for all similar devices offered by the manufacturer?	
5. Is the installed version of the operating system currently deployed with this device the most current production version, or no more than one major revision behind the most current available?	
6. Is the operating system currently deployed with this device scheduled for future production releases?	
Total Rating Points	

3. Operating Systems Security refers to a security functionality that is available with the Operating System (must be answered relative to responses in 2. Operating Systems.)

Score 1 Rating Point for a "Yes" answer	**Yes**
1. Do the operating system security services align with the AZ EA Target Security Architecture?	
2. Does the operating system security allow for logging and the security controls for applications, platform, and network levels to be integrated to reduce and eliminate redundancies?	
3. Does the operating system support access, authentication, and authorization techniques as defined in the AZ EA Target Security Architecture and related standards?	
4. Does the operating system allow for an integrated LDAP directory service?	
5. Does the operating system allow for all security updates to be pushed to, or accepted by, all associated devices?	
6. Does the operating system allow for logging and restriction, including preventing end-user override, of particular functions or services, such as non-essential or redundant services, communication options that are susceptible or prone to abuse, and operating-system-level utilities?	
7. Can extraneous services, open ports, etc., be easily removed from "default installations of the operating system" and prevented from returning when the operating system is upgraded?	
Total Rating Points	

4. Open Standard Interfaces and Drivers refer to a device's capability to adhere to open-system-standard interface specifications and to utilize device drivers that use IEEE and industry de-facto standard protocols and formats.

Score 1 Rating Point for a "Yes" answer	**Yes**
1. Does the device utilize target network standards for communication protocols?	
2. Is the device capable of being configured, managed, and maintained using standard SNMP-based management tools?	
3. Is the device capable of utilizing open-standard drivers that employ IEEE-interfaces and industry de-facto standard software drivers?	
4. Are multiple, off-the-shelf, peripheral devices that conform to open-system-standards and that utilize "de-facto" standard drivers available for this device?	
Total Rating Points	

ATTACHMENT B. STATE OF ARIZONA "AS-IS" PLATFORM ASSESSMENT

Please refer to http:/gita.state.az.us/enterprise_architecture/platform_assess.htm for latest "as-is" platform ratings.